AIR WAR COLLEGE

AIR UNIVERSITY

ENHANCING NATIONAL SECURITY COOPERATION POLICY WITH REMOTELY PILOTED AIRCRAFT

by

Ken Callahan, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2012

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Ken Callahan is a U.S. Air Force pilot assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from the U.S. Air Force Academy in 1992 with a Bachelor of Science degree in History, Troy State University in 1993 with a Masters of Management, and University of Phoenix in 2007 with a Doctorate of Management. He earned his pilot wings in 1995 and has over 2,700 flying hours in the C-141, C-5, T-37, and MQ-1. He has served at USTRANSCOM and is a graduated squadron commander.

Abstract

The 2010 National Security Strategy directs the Defense Department to enhance relationships with old allies and create new partnerships with other countries seeking to defeat Al Qaeda.[1] The Department of Defense uses nation and region-specific security cooperation programs to promote stability, prepare for coalition operations, exchange information and intelligence, and ensure strategic access when needed. Air Force Intelligence Surveillance and Reconnaissance Remotely Piloted Aircraft systems have the ability to enhance all of the outcomes desired by security cooperation programs, but are currently restricted by the Missile Technology Control Regime (MTCR), network security concerns and the lack of global operating standards. Reevaluating MTCR restrictions, improving network security, and standardizing global procedures and regulations will enhance security cooperation programs and improve overall national defense.

Introduction

The global security environment has changed dramatically since the terrorist attacks of September 11, 2001. The new environment is characterized by a spectrum of threats ranging from non-state actors based in failed states,[2] to the rise of new regional powers, to continued concern about the spread of weapons of mass destruction.[3] Responding to these threats requires a new approach directed by our national security strategy that includes "an adaptive blend of diplomacy, development, and defense"[4] and a realization that the United States must learn to accept partnerships of varying degrees of commitment to ensure our own security.[5] Building partnerships includes strengthening relations not only with like-minded democratic allies but also with nations that have "little in common except for the desire to defeat al-Qaeda and its affiliates and adherents."[6]

From a military perspective, building a spectrum of security partnerships requires the Department of Defense to enhance nation-specific security cooperation programs in an effort to leverage their unique capabilities. However, in the new security environment, nation-specific programs must be linked to a global security strategy that responds to increasingly global threats. Security cooperation programs should promote United States security interests, improve allied and partner capacity, facilitate information and intelligence sharing, and provide access to forward basing and en route infrastructure.[7] Each of these criteria are easy to understand, but increasingly difficult to apply to the wide spectrum of complex relationships ranging from strong traditional allies to weak partnerships with nations who wish to defeat radical ideology but have little else in common with the United States.[8]

Two unique technology systems that can achieve Department of Defense security cooperation goals across a spectrum of tailored relationships are the Air Force's fleet of MQ-1

Predator and MQ-9 Reaper intelligence, surveillance, and reconnaissance (ISR) remotely piloted aircraft (RPA). These ISR RPA systems can be globally postured and regionally focused in a manner that enhances global security cooperation efforts. Unfortunately, there is not currently an overarching strategic plan in place to provide specific nations with ISR RPA capabilities to promote security cooperation. In addition, the 34 member international body Missile Technology Control Regime (MTCR) led by the United States has placed restrictions on the proliferation of ISR drones in an effort to limit the spread of vehicles that can deliver weapons of mass destruction.[9] Despite this restriction, the United States should reconsider its position on the proliferation of ISR RPA systems and include these systems in a global security cooperation plan that accounts for a wide-range of nation-to-nation relationships.

The purpose of this research paper is to provide a baseline discussion for how Air Force MQ-1 and MQ-9 ISR RPA platforms can enhance security cooperation. Following a brief overview of Department of Defense security cooperation programs, a specific approach to integrating MQ-1 and MQ-9 ISR RPA systems across a range of partnerships will be proposed. It is recognized that there are current prohibitions in place that prevent the proliferation of these systems. These prohibitions will be discussed as challenges to United States strategic choices and will be considered in the recommendation portion of this paper.

Security Cooperation

Joint Publication 3-0, *Joint Operations* discusses security cooperation and military engagement activities together as the means by which the Department of Defense interacts with other nations to ensure security, deter conflict, and enable future contingency operations. Joint Publication 3-0 defines security cooperation as:

> All DOD interactions with foreign defense and security establishments to build defense relationships that promote specific US security interests, develop allied

> and friendly military and security capabilities for internal and external defense and for multinational operations, and provide US forces with peacetime and contingency access to the HN [host nation]."[10]

Likewise, Joint Publication 3-0 states, "Military engagement occurs as part of security cooperation, but also extends to interaction with domestic civilian authorities."[11] For simplicity, throughout this discussion, the term *security cooperation* will include interactions with both military and domestic civilian authorities.

Joint Publication 3-22, *Foreign Internal Defense* Figure I-4 lists fifteen activities with the last being "other programs and activities,"[12] implying some leeway. However, despite the multiple number of activities that can occur under the umbrella of security cooperation, all of the activities can be grouped under four broad categories: stability operations, preparing for coalition operations, information and intelligence sharing, and strategic access.[13] Grouping all the security cooperation activities into these four broad categories is non-doctrinal, but forms a good framework for consideration.

Security Cooperation Activities			
Stability Operations	**Preparing For Coalition Ops**	**Information and Intelligence Sharing**	**Strategic Access**
- Counter-narcotics Assistance - Counter/Non-Proliferation - Defense Support to Public Diplomacy - International Armaments Cooperation - Security Assistance - Humanitarian Assistance	- Multinational Education - Multinational Exercises - Multinational Experimentation - Multinational Training	- Intelligence Cooperation - Information Sharing	- Defense & Military Contacts - Facilities & Infrastructure Projects

Stability Operations

The primary purpose of security cooperation programs is to promote US interests abroad. In most situations, US interests are best served by ensuring the stability of allied and partner

nations and the global regions those nations are in. Joint Publication 3-07, *Stability Operations* defines stability operations as:

> …various military missions, tasks, and activities conducted outside the US in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.[14]

Security is a key part of stability operations and a lack of security often generates the need for stabilization operations to begin.[15] Generally, security is thought of as an external consideration or "a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences."[16] Yet, security concerns may also arise from internal sources such as an insurgency, organized crime, or drug trafficking.

When the US has an alliance with another nation, stability and security support arrangements are generally codified in a treaty or formal agreement. However, when the US deals with less formal partners, a consideration of US interests must be made on a case-by-case basis. In addition, the US must evaluate the motives of a partner nation. As William Lambert notes, a partner nation's definition of security might be different than that of the US. The US may seek to protect a nation from external threats while the leadership of the partner nation may simply want to stay in power. A controlling regime may view with more concern threats from internal rather than external sources.[17] Under such circumstances, careful consideration must be given to supporting a country that may use support (especially military support) for an unintended purpose.

Preparing for Coalition Operations

Former Secretary of Defense Robert Gates highlighted the importance of building allied partner capacity to meet the challenges of the current security environment during his tenure as

head of the Defense Department. He noted that the effectiveness and credibility of the US would rely on the effectiveness and credibility of local partners. Gates commented:

> This strategic reality demands that the US government get better at what is called *building partner capacity*: helping other countries defend themselves or, if necessary, fight alongside US forces by providing them with equipment, training, or other forms of security assistance.[18]

In order to accomplish Gates' vision, the US must provide allies and partner nations with both the equipment and the training required to operate in a coalition environment. In many cases this task requires the US to transform and optimize foreign militaries in an effort to raise their capabilities to a level where they can effectively contribute to an operation.[19] Long-term allied nations (for example, many NATO partners) already have significant capabilities, but less developed partners may require a long-term investment to raise their capabilities to an effective level.

Information and Intelligence Sharing

Since September 11th, 2001, the US has placed a greater interest on information and intelligence sharing with foreign governments. The 2010 National Security Strategy states, "…our intelligence and law enforcement agencies must cooperate effectively with foreign governments to anticipate events, respond to crises, and provide safety and security."[20] Unlike security, stability, and coalition warfare, the US is not always the strongest partner when it comes to information and intelligence gathering. The 2008 National Defense Strategy notes, "Often our partners are better positioned to handle a given problem because they understand the local geography, social structures, and culture better than we do or ever could."[21] Due to the strengths of our allies and partners, it is vital to US interests to establish structures and agreements to facilitate information and intelligence exchanges.

Responsibility for information and intelligence sharing protocols is given to commanders, but restricted by law. Joint Publication 3-0 highlights the importance of information and intelligence exchanging:

> The sharing of information with relevant USG [US government] agencies, foreign governments and security forces, inter-organizational partners, NGOs [non-government organizations], and members of the private sector, has proved vital in recent operations. Commanders at all levels should determine and provide guidance on what information needs to be shared with whom and when. DOD information should be appropriately secured, shared, and made available throughout the information life cycle to appropriate mission partners to the maximum extent allowed by US laws and DOD policy. Commanders, along with their staffs, need to recognize the criticality of the information-sharing function at the outset of complex operations and not as an afterthought.[22]

Strategic Access

The 2010 National Military Strategy states, "Global posture remains our most powerful form of commitment and provides us strategic depth across domains and regions."[23] Security cooperation programs improve global posture by engaging host nations in order to obtain strategic access to facilities and sovereign space during both peacetime and contingency operations.[24] Additionally, strategic access includes making contacts with appropriate local agencies, establishing support contracts and improving host nation facilities when necessary. This type of strategic access to allied and partner nations frequently requires enduring relationships based on trust and commitment to long-term security. Fortunately, the Air Force now possesses a flexible technology that can permit tailored security cooperation across all four broad areas with partners of diverse capabilities and capacities.

ISR RPA Systems

There are many tools available to conduct security cooperation activities, but few have the ability to conduct all security cooperation activities as comprehensively as Air Force ISR RPAs. Although the Air Force ISR RPA portfolio is large and growing, the most commonly

known and widely requested systems are the MQ-1 Predator and the MQ-9 Reaper. Both the Predator and the Reaper are unique because they are *systems* that are more extensive than the aircraft itself.

The MQ-1 and MQ-9 systems are complex, but the main elements are the aircraft, ground control station (flight controls), video distribution and exploitation system, and data-links. The aircraft are relatively low technology airframes with a high resolution camera. In addition to the camera, the MQ-1 and MQ-9 are designed to carry weapons to include the AGM-114 Hellfire laser guided missile and the GBU-12 500-pound laser guided bomb. The aircraft can be modified to carry additional payloads at the expense of fuel and overall endurance.[25]

The MQ-1 and the MQ-9 systems are remotely piloted from a ground control station. The ground control stations consist of the same hardware for both the MQ-1 and the MQ-9, but each requires different software. The basic crew for the MQ-1 and MQ-9 consists of a pilot (responsible for flying the aircraft) and a sensor operator (responsible for operating the camera). A third crew member, mission intelligence coordinator, is added when needed to operate in a complex tactical environment.[26]

Both the MQ-1 and the MQ-9 systems can provide real-time full motion video direct to the battlefield or to a command center anywhere in the world. This allows command and control elements to maintain some direct awareness of and remote access to the battlefield. Information and intelligence gathered during operations can also be shared and exploited real-time permitting decisions to be made at a faster rate.[27]

Data-links comprise many different systems available to control and monitor the aircraft and its payload. MQ-1 and MQ-9 RPAs can be controlled using various technology and methods to fit the needs of the mission being performed. The control technology and methods can be

tailored to balance information access with security, and autonomy with failsafe control, as desired by the commander.

Types of Control

There are four basic ways of operating MQ-1 and MQ-9 RPAs: pre-programmed missions, line-of-site control, beyond line-of-site satellite control, and remote split operations. Pre-programmed missions are uploaded to a computer in the aircraft which then flies the programmed mission until a new mission is re-loaded. Often, emergency missions are pre-programmed in the event the primary control link is broken so the aircraft can fly to a specific location where another control link can be established. Pre-programmed missions are not usually the primary method of control because they limit tactical interactivity.[28]

Line-of-site control requires a ground based signal to be sent to an aircraft. This type of control limits the range of the aircraft due to the strength of the control signal, terrain, and atmospheric conditions, but does not limit the RPAs endurance. Line-of-site control is especially useful for base defense operations and limited range but high endurance targets (urban or border patrol). In addition, line-of-site control tends to be more responsive and less expensive that satellite control options.[29]

Beyond line-of-site control uses a satellite link to fly the aircraft. Typically, a line-of-site signal will be used to launch the aircraft and then the crew will establish a secure satellite control link to increase the range of the aircraft. Using this type of control, aircraft range is limited only by fuel and satellite signal limitations. This type of control is very useful with limited airfield infrastructure and geographic challenges (large border areas, difficult terrain, remote locations, etc.).[30]

Remote split operations expand on the beyond line-of-site concept by adding an additional crew in a different location. Using this type of control, a crew launches an aircraft using line-of-site control and then passes control via a hand-off procedure to a flight crew at a different location using a secure satellite control link. The US currently uses this construct effectively to fly its ISR RPA fleet and the advantages are numerous. Using remote split operations, a CONUS-based crew can fly an RPA anywhere in the world. CONUS basing improves support structures, limits risk to aircrews, and permits real-time reallocation from one theater of operations to another within a short period of time.[31]

ISR RPAs and Stability Operations

The MQ-1 and MQ-9 ISR RPA systems are well suited for a variety of stability operations in allied and partner nations. The 2010 Quadrennial Defense Review states, "Long-dwell UASs [Unmanned Aerial Systems] such as the Predator, Reaper, and other systems, have proven to be invaluable for monitoring activities in contested areas, enhancing situational awareness, protecting our forces, and assisting in targeting enemy fighters."[32] An allied or partner nation could easily realize the same benefits if trained and equipped with MQ-1 and MQ-9 aircraft. In addition, the 2010 Quadrennial Defense Review notes, "Terrorist groups seek to evade security forces by exploiting ungoverned and under-governed areas as safe havens from which to recruit, indoctrinate, and train fighters, as well as to plan attacks on US and allied interests."[33] Because of their ability to monitor such areas, both the MQ-1 and the MQ-9 provide a capability for a country to deny terrorist access to ungoverned space.

In addition, the MQ-1 and MQ-9 have proven to be useful in humanitarian assistance missions. After the Haiti earthquake in 2010, the United States provided MQ-1 support to monitor supply movements and direct the limited Haitian police force to troubled areas.

Although this operation was flown using US crews employing remote split operations control, if trained and equipped, Haitian forces could have flown the operation using line-of-site control directly from their own airfield.[34]

ISR RPAs and Preparing for Coalition Operations

Perhaps the most unique aspect of ISR RPAs is the ability for a crew to fly an aircraft from anywhere in the world. This has great utility for training with allied partners. For example, utilizing remote split operations, a NATO ally could participate from their home station in an exercise being conducted in United States military training airspace. This type of training would greatly enhance interoperability of forces for both peace and wartime coalition operations. Conversely, a crew from the United States could get real-time training in European airspace without leaving CONUS. This type of training is much less expensive than deploying squadrons for military training, but still realizes the same benefits of multi-national training exercises.

Information and Intelligence Sharing

Information and intelligence sharing represents the greatest potential gains in security cooperation for the United States. Local partners often know the area, terrain, and customs better than American analysts and can provide crucial inputs about what to look at and when.[35] In addition, when an MQ-1 or MQ-9 video feed is distributed across a network, command centers around the globe can simultaneously access information and full-motion video real-time. In Haiti, full motion video was shared directly with government and non-government agencies in both the United States and Haiti. This provided good awareness of the problem by allowing relief participants to view stricken areas, determine the extent of damage, and prioritize relief efforts.[36]

In addition, intelligence sharing is valuable during allied and coalition operations and can be restricted to permit access from secure areas and approved partners. One approach to intelligence sharing may be to have a US air crew fly the RPA but give an allied or partner nation access to the video feed and exploitation resources. The ally or partner nation can even participate in the targeting or maneuvering of the aircraft or sensor through direct communication with a US command center or the crew. In addition, an allied or partner nation might also be able to fly the aircraft and provide intelligence back to the United States in the same manner. Different relationships and capabilities with the host country will dictate different approaches.

Strategic Access

Obtaining strategic access to regions, airspace, and host-nation facilities is an important part of the United States global engagement strategy. The 2011 National Military Strategy states, "With partner nation support, we will preserve forward presence and access to the commons, bases, ports, and airfields commensurate with safeguarding our economic and security interests worldwide."[37] An integrated RPA plan can facilitate and improve the forward basing options.

For example, a country located in a region sensitive to a large presence of US military forces could be equipped with lower signature MQ-1s or MQ-9s as part of a foreign military sales package. The host-nation could then fly the aircraft to observe areas of interest like a disputed border or ungoverned territory, and the video feed could be sent to a coalition command center for exploitation. Another alternative application would be to ask the allied or partner nation to launch and recover the aircraft while US crews fly the missions from CONUS. This arrangement would leverage the host nation's ability to work airspace, logistics, and billeting

issues, but give the US access to the region. In either example, the approach taken can be tailored to meet the needs of the mission.

Challenges

Despite the advantages of using ISR RPAs to enhance security cooperation, there are significant challenges the Air Force must overcome before MQ-1 and MQ-9 systems can be integrated into security cooperation programs. Three specific challenges are the Missile Technology Control Regime's (MTCR) export limitations, network security, and system standardization. Each issue requires significant changes by the Air Force, and the Department of Defense before ISR RPAs can be exported to global allies and partners.

MTCR Restriction

The MTCR was established in 1987 by the United States, Canada, France, West Germany, Italy, Japan and the United Kingdom to "prevent the proliferation of missiles and unmanned aerial vehicle capable of delivering nuclear weapons."[38] In 1993, the MTCR expanded its charter to limit the "proliferation of missile delivery systems for all weapons of mass destruction."[39] Since the creation of the organization, the MTCR has grown to 34 partner nations. Currently, the MTCR does not permit the sale of MQ-1 or MQ-9 aircraft to other nations because these weapons systems have the capability of delivering a 500-kg payload to a range of 300-km. This restriction has been in-place for over 20 years but will be reconsidered at the next MTCR meeting in April 2012.

The MTCR restrictions on the export of ISR RPA technology are problematic for using MQ-1 and MQ-9 RPAs as part of security cooperation programs. The 2005 Air Force RPA strategic vision document noted the restrictions and advocates their removal:

> The Air Force must continue to address RPA and UAV export policy. The sale of US-manufactured, interoperable RPAs and UAVs to key allies and foreign

> partners enhances coalition capability, and an integrated production strategy provides advantages to the US industrial base. Currently, the Missile Technology Control Regime (MTCR) limits the export of the MQ-1 Predator, MQ-9 [Reaper], and RQ-4 Global Hawk, severely constraining RPA security cooperation activities with allies and foreign partners. The Air Force must continue to advocate updates to the MTCR and the US government export policy to fully develop interoperable coalition capabilities that support US national security objectives.[40]

Network Security

The second challenge for the Air Force to overcome prior to exporting MQ-1s and MQ-9s is network security. As Pentagon spokesman Bryan Whitman noted in 2009:

> Every capability comes with its advantages, disadvantages, benefits as well as potential weaknesses. As you develop those (technologies) you have to be mindful of how the enemy can counteract any technology that you have. That's why you always have a constant review process in place to not only improve that capability but address any vulnerabilities it may have.[41]

In the past five years, there have been two network security vulnerabilities publicly acknowledged and fixed by the Air Force in the ISR RPA system. The first was the discovery that insurgents in Iraq had found a way to hack into data feeds and monitor full motion video from MQ-1 aircraft. In December 2009, a Pentagon spokesman acknowledged the breach and indicated the problem had been fixed.[42] A second vulnerability was discovered in September 2011, when a credential-stealing virus was discovered on ground control station hard drives at Creech Air Force Base. The Air Force described this virus as a *nuisance* and reportedly isolated and removed the virus from the system.[43]

Unfortunately, network security will only get more difficult as allies and partners are given access to the system. However, access to the network is only required when RPAs are fully integrated and satellite technology is in-use. By limiting integration or employing line-of-site control, RPAs can be isolated from the network. Implementing restrictions on integration and

control methods increases network security but decreases the overall effectiveness of the systems.

System Standardization

System standardization is another significant issue the Air Force must address prior to implementing a comprehensive security cooperation program with ISR RPAs. As noted with network security, standardized equipment, network monitoring, and security protocols are important to the health and effectiveness of the entire system. In addition, the Federal Aviation Administration has raised specific concerns over the lack of standardization with displays, controls, response to system failures, crew composition, and crew qualifications. Although these concerns are specific to national airspace in the United States, many of the same concerns will need to be addressed to operate in international airspace.[44]

Recommendations and Conclusions

The 2010 National Security Strategy directs the Defense Department to enhance relationships with old allies and create new partnerships with other countries seeking to defeat Al Qaeda.[45] The Department of Defense uses nation and region-specific security cooperation programs to promote stability, prepare for coalition operations, exchange information and intelligence, and ensure strategic access when needed. Air Force ISR RPA systems have the ability to enhance all of the outcomes desired by security cooperation programs, but are currently restricted by the MTCR, network security concerns, and the lack of global operating standards. In order to overcome the current challenges and limitations, the Air Force should consider advocating three recommendations.

Recommendation #1

The United States should open discussion with MTCR members to reconsider the ban on the proliferation of ISR RPA systems. Although MTCR concerns about delivery systems for weapons of mass destruction are shared by the United States, MQ-1 and MQ-9 ISR RPA systems are not the most threatening delivery platforms. The MQ-1 and MQ-9 systems do not employ stealth technology or self-defense capabilities and are relatively slow moving vehicles that can easily be defeated by air defense systems.[46] The security benefits gained by exporting MQ-1s or MQ-9s outweigh the limited risk of them possibly being used to deliver a weapon of mass destruction.

In addition, nations with the ability to manufacture weapons of mass destruction are likely to have the ability to manufacture their own unmanned platforms. For example, Iran, India, Russia, Pakistan, China and the European Union have already built and marketed unmanned aircraft and are benefitting from national sales and partnerships with interested nations.[47] Restricting exports of unmanned aircraft systems among friendly nations does not eliminate the threat from more aggressive nations and damages United States efforts to establish security cooperation relationships.

Recommendation #2

In the absence of a fully secure network, the Air Force should pursue the sale of MQ-1 and MQ-9 systems with limited line-of-site control technology that would isolate partners from secure networks. Although limiting access will reduce the ability for partner nations to integrate with the United States, some limited security cooperation goals can still be accomplished. For example, restricting network access will prevent nations from participating in intercontinental

multinational training and exercises but will permit stability operations to be performed by the host nation.

Recommendation #3

The United States is the global leader in unmanned systems, but standardized operating procedures and regulations have not caught up with the rapid growth of the program. The Air Force should take the lead in developing operating procedures that are acceptable to other services, the Federal Aviation Administration, and the international airspace system. By leveraging its leadership position in unmanned systems, the Unites States has the opportunity to pioneer standards for the global community that are in our national interest and include safety, equipment specifications, and crew qualifications. If the United States does not take the lead in exporting unmanned systems, other nations (to include adversaries) will. By forfeiting the leadership role, the United States will have less influence in establishing global rules and standardization. In combination, reevaluating MTCR restrictions, improving network security, and standardizing procedures and regulations will strengthen security cooperation with other nations and improve overall national defense.

Bibliography

432d Air Expeditionary Wing Mission Briefing, Creech Air Force Base, NV, June 2011.

Dyekman, Gregory. "Security Cooperation: A Key to the Challenges of the 21st Century." Army War College. Carlisle, PA, November 2007.

Gates, Robert M. "Helping Others Defend Themselves." Foreign Affairs: May/Jun 2010, Vol. 89, Issue 3, p. 2-6.

International Institute for Strategic Studies, "*Rumblings Precede 25th Missile-Control Meeting, Strategic Comments*," 17-3, 1-3, Mar 2011. Retrieved on September 15 2011 at http://dx.doi.org/10.1080/1356788.2011.581852.

Joint Publication 3-07, *Stability Operations*, September 29, 2011.

Joint Publication 3-22, Foreign Internal Defense, July 12, 2010.

Kelley, Terrence, Jefferson Marquis, Cathryn Thurston, Jennifer Moroney, and Charlotte Lynch. *Security Cooperation Organizations in the Country Team: Options for Success*. RAND Technical Report, 2010.

Lambert, William. *US-Central Asian Security Cooperation: Misunderstandings Miscommunications & Missed Opportunities*, Security Assistance: US and International Historical Perspectives, eds. Kendall Gott and Michael Brooks, Combat Studies Institute Press, Fort Leavenworth Kansas.

McCarley, Jason and Christopher Wickens, "Human Factors Concerns in UAV Flight," Institute of Aviation, Aviation Human Factors Division, University of Illinois, Urbana-Champagne IL, retrieved on December 4, 2011 from http://www.FAA.gov.

Nikitin, Mary Beth, Paul Kerr, and Steven Hildreth. *Proliferation Control Regime: Background and Status Congressional Research Service*, October 2010.

Reveron, Derek. *Exporting Security: International Engagement, Security Cooperation, and the Changing Face of the U.S. Military*. Washington D.C.: Georgetown University Press, 2010.

Schachtman, Noah, "Air Force Insists: Drone Cockpit virus Just a Nuisance," *Wired Magazine*, October 2011, Retrieved 4 December 4, 2011from http://www.wired.com/dangerroom/2011/10/drone-virus-nuisance.

Stewart, Phil. "US Military Drone Security Breach Fixed," *Reuters*, December 17 2009.

Theis, Douglas G. "Airpower Security Cooperation as an Instrument of National Power: Lessons fro Iraq from the Cases of Pakistan and Egypt." *Air & Space Power Journal*: Fall 2009.

The U.S. Air Force Remotely Piloted Aircraft and Unmanned Aerial Vehicle Strategic Vision. Washington D.C.: Department of the Air Force, 2005.

U.S. President of the United States. *National Security Strategy*. Washington D.C.: White House, May 2010.

U.S. President of the United States. *National Strategy for Counterterrorism*. Washington D. C.: White House, June 2011.

U.S. Department of Defense. *National Defense Strategy*. Washington D.C. June 2008.

U.S. Department of Defense. *The National Military Strategy of the United States of America*. Washington D.C. February 2011.

U.S. Department of Defense. *Quadrennial Defense Review Report*. Washington D.C. February 2010.

Willson, J. R., "UAV Worldwide," *Aerospace America,* April 2009, retrieved from: http://www.aiaa.org/aerospace/images/articleimages/pdf/UAVs_APR2009.pdf on December 6 2011.

[1] *National Security Strategy*, 2010.
[2] Robert Gates, *Helping Others Defend Themselves*. Foreign Affairs. May/Jun 2010, Vol. 89 Issue 3, p. 2-6.
[3] National Defense Strategy, 2008, p. 1.
[4] Department of Defense, *The National Military Strategy of the United States of America*. 2011, p. 1.
[5] *National Strategy for Counterterrorism*, Jun 2011, p. 6.
[6] Ibid, p. 7.
[7] Derek Reveron, *Exporting Security: International Engagement Security Cooperation and the Changing Face of the U.S. Military*. Georgetown University Press (Washington D.C., 2010), p. 105.
[8] National Strategy for Counterterrorism, Jun 2011, p. 6.
[9] Missile Technology Control Regime official website, Feb 2012, http://www.mtcr.info/english/guidelines.html
[10] Joint Publication 3-0, p. V-10.
[11] Ibid.
[12] Joint Publication 3-22, p. I-11.
[13] Derek Reveron, p. 105.
[14] Joint Publication 3-07, p. I-2.
[15] Ibid, p. I-19.
[16] William Lambert, *US-Central Asian Security Cooperation: Misunderstandings Miscommunications & Missed Opportunities*, Security Assistance: US and International Historical Perspectives, ed. Kendall Gott and Michael Brooks, Combat Studies Institute Press, Fort Leavenworth Kansas, 2006, p. 127.
[17] Ibid.
[18] Robert Gates, p. 2.
[19] Derek Reveron, p. 105.
[20] National Security Strategy, 2010, p. 17.
[21] National Defense Strategy, 2008, p. 8.
[22] Joint Publication 3-0, III-14.
[23] The National Military Strategy of the United States of America, 2011, p. 10.
[24] Joint Publication 3-0.
[25] 432d Air Expeditionary Wing Mission Briefing, Creech Air Force Base, NV Jun 2011.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Department of Defense, Quadrennial Defense Review Report, Feb 2010, p. 22.
[33] Ibid, p. 27.
[34] 432d Air Expeditionary Wing Mission Briefing, Creech Air Force Base, NV, Jun 2011.
[35] National Defense Strategy, 2008, p. 8.
[36] Ibid.
[37] The National Military Strategy of the United States of America, 2011, p. 10.
[38] Mary Beth Nikitin, Paul Kerr, and Steven Hildreth, Proliferation Control Regime: Background and Status, Congressional Research Service, October 2010, p. 33.
[39] Ibid, p. 34
[40] The Secretary of the Air Force, *The US Air Force Remotely Piloted Aircraft and Unmanned Aerial Vehicle Strategic Vision*, 2005 (Washington, DC: Government Printing Office) 2005, p. 34.
[41] Phil Stewart, "US Military Drone Security Breach Fixed," *Reuters*, December 17 2009, http://www.reuters.com/assets (accessed 4 December 2011).
[42] Ibid.

[43] Noah Schachtman, "Air Force Insists: Drone Cockpit Virus Just a Nuisance," *Wired Magazine*, October 2011, http://www.wired.com/dangerroom/2011/10/drone-virus-nuisance/ (accessed 4 December 2011).
[44] Jason S. McCarley and Christopher D. Wickens, "Human Factors Concerns in UAV Flight," Institute of Aviation, Aviation Human Factors Division, University of Illinois, Urbana-Champaign IL, retrieved from http://www.FAA.gov on 4 December 2011.
[45] National Security Strategy, 2010.
[46] 432d Air Expeditionary Wing Mission Briefing, Creech Air Force Base, NV Jun 2011.
[47] J.R. Willson, "UAV Worldwide," *Aerospace America*, April 2009, retrieved from: http://www.aiaa.org/aerospace/images/articleimages/pdf/UAVs_APR2009.pdf on December 6 2011.